## Primary Roles and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**NIH Senior Official for Privacy (SOP) -** The OPDIV official who serves as the primary party and champion responsible for the implementation of privacy requirements and controls.

- Support the roles and responsibilities of the HHS Senior Agency Official for Privacy as appropriate;
- Develop and implement an IT Privacy Program consistent with Department policy and requirements set forth in the Federal Information Security Management Act and Agency Privacy Management Report;
- Develop/incorporate NIH privacy guidance into NIH and system-level documentation to ensure consistency with Department policy and guidance;
- Recommend allocation of proper resources to senior level officials with budgetary authority to mitigate privacy weaknesses;
- Coordinate with NIH budgetary offices to ensure Privacy Impact Assessment and Systems of Records Notice activities are included as part of Exhibit 300 development;
- Coordinate with the NIH Chief Information Security Officer to report on the status of the organization's information privacy program, including progress of remedial actions;
- Ensure that PIAs are completed for all NIH systems and review all completed PIAs for promotion to the Department;
    - Receive the PIAs from the PIA author;
    - Conduct quality reviews of PIAs for completeness and accuracy, and identify any privacy weaknesses;
    - Submit the PIAs to the Department's Senior Agency Official for Privacy once complete, or return them back to the PIA author for revisions;
    - Track and maintain all PIA activities in the current ProSight FISMA tool;
    - Keep management informed of any PIA resource needs and identified areas of privacy weakness;
- Coordinate with the Website Owners/Administrators to ensure that web-based privacy compliance requirements are met across the Department;
- Coordinate with the NIH CISO and privacy stakeholders to ensure that privacy awareness training and activities are incorporated as part of contractor responsibilities on an annual basis;
- Coordinate with the NIH CISO to ensure that adequate and appropriate privacy awareness training and activities are provided to employees and other NIH privacy stakeholders on an annual basis;

- Review and approve NIH Privacy Management Section of the Office of Management and Budget FISMA and Privacy Management Report;
- Comply with and maintain the privacy goals of the President's Management Agenda;
- Coordinate with members of the NIH Incident Response Team to report suspected incidents involving personally identifiable information;
- Coordinate with the NIH Privacy Contacts to support SORN and A-130 activities;
- Coordinate with the NIH CISO, NIH Police and members of the NIH Incident Response Team to develop and support PII incident standard operating procedures to effectively report suspected PII breaches according to Department and OMB Guidance; and
- Manage and certify an inventory of all current and proposed NIH investments that contain a privacy control component.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**NIH Privacy Act Officer –** The OPDIV official responsible for overall compliance with the Privacy Act.

- Maintain awareness of privacy laws, regulations, and Privacy Act issues within NIH;
- Oversee, develop and implant NIH's compliance with the Privacy Act;
- Coordinate as necessary with the NIH Senior Official for Privacy to ensure 90% of systems subject to the Privacy Act have a Systems of Records Notice to comply with the President's Management Agenda;
- Ensure that SORNs meet the requirements of the Privacy Act, are reported biennially in accordance with the requirements of the Privacy Act, and submitted to the Federal Register for publication prior to use;
- Maintain an NIH SORN website to post current SORNs per the guidance of the Department Privacy Act Officer; and
- Support the NIH Senior Official for Privacy and Chief Information Security Officer in completing required reviews as defined as part of OMB Circular A-130, *Management of Federal Information Resources*.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**NIH Chief Information Security Officer (CISO) –** The OPDIV official responsible for the NIH Information Security Program.

- Coordinate with the NIH CIO, SOP and other NIH and HHS officials, etc., in the event of a breach to ensure that proper reporting and remedial actions are taken;
- Maintain and oversee the NIH Incident Response Team;
- Coordinate with the U.S. Computer Emergency Response Team to report suspected incidents involving PII;
- Assist the NIH Senior Official for Privacy in developing the organization's information privacy program;
- Ensure that all federally mandated information security measures in support of privacy are implemented;
- Coordinate with the NIH SOP to integrate and implement privacy into security policies, procedures, and practices consistent with Departmental requirements;
- Assist in the incorporation of security and privacy considerations within acquisition documents, and help to ensure that contractor compliance is maintained;
- Assist the NIH SOP to develop and maintain a framework to facilitate the development and maintenance of PIAs;
- Coordinate with the NIH SOP to incorporate general privacy awareness and role-based training activities into parallel security training;
- Ensure that privacy awareness and education is mandatory for all NIH employees and contractors who are using, operating, supervising, or managing NIH computer systems;
- Coordinate privacy reporting activities as mandated by federal privacy legislation and Office of Management and Budget Guidance.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**NIH Forms Officer –** The OPDIV official responsible for establishing new NIH forms or revising existing NIH forms.

- Advise when NIH data collection forms are governed by the Privacy Act;
- Advise when NIH forms require a Privacy Act Notification Statement; and
- Coordinate with the IC Privacy Coordinator on the accuracy of a Privacy Act Notification Statement and the special requirements for use of the SSN on forms created by, and for the use of ICs and individuals.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Privacy Coordinator –** The Institute/Center of Office official who serves as the liaison between IC staff and both the NIH Senior Official for Privacy and the NIH Privacy Act Officer, on privacy and Privacy Act issues.

- Maintain awareness of privacy laws, regulations, and issues;
- Advise IC System Owners/Managers and staff on issues pertaining to the Privacy Act and related privacy legislation and policy;
- Distribute privacy memoranda and bulletins to NIH personnel so that they are informed of current OMB, HHS and NIH privacy policies and procedures;
- Ensure that System Owners/Managers maintain privacy notices, policies, and procedures for all applicable IT systems as appropriate;
- Respond to requests for access to records from individuals whose personally identifiable information resides in a Privacy Act system of records;
- Assist NIH CISO and IC ISSO in performing security reviews of PA systems;
- Coordinate with the NIH SOP on the annual requirement, and satisfactory completion of, privacy awareness training for IC staff and contractors;
- Review and clear Privacy Impact Assessments for promotion to the NIH SOP;
- Coordinate with the NIH Privacy Act Officer on records requested under the PA, requests for OMB clearance, requests for the use of persistent cookies, web page compliance, the bi-annual update of SORNs, the completion of the bi-annual PA report, etc.; and
- Attend the monthly Privacy Coordinator Group meetings.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Privacy Act System Owner/Manager –** The Institute/Center or Office official responsible for a group of records under the control of the agency where information is retrieved by the name of the individual, by some identifying number or symbol, or by other identifiers assigned to the individual, who will (in coordination with knowledgeable privacy and security personnel as needed):

- Serve as a point of contact for the system to whom privacy issues may be addressed;
- Collect, modify, use, and disclose the minimum PII necessary to complete the mission-related, required and/or permitted program task consistent with organizational policy;
- Keep track of the location of Privacy Act records;
- Approve/deny/track access to, and amendments of, records;
- Ensure records are complete, accurate, timely and relevant;
- Ensure that system users are made aware of their privacy responsibilities when accessing systems that contain personal information;
- Ensure data collection forms include a Privacy Act Notification Statement;
- Submit Privacy Act annual report data to the IC Privacy Coordinator;
- Inform staff of the annual requirement to take privacy awareness training;
- Comply with the NIH Records Control Schedule;
- Coordinate with appropriate NIH privacy stakeholders and identify additional resources and staff necessary to complete system Privacy Impact Assessments.

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Information Technology (IT) System Owner/Manager – The Institute/Center or Office official responsible for the development, operation and/or maintenance of an information technology system defined as an organized assembly of IT resources and procedures integrated and regulated by interaction or interdependence to accomplish a set of specified functions.**

**A General Support System (GSS)** is an interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN), including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center and its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). (Defined in Office of Management and Budget (OMB) Circular A-130, (A)(2)(c).) Examples include, but are not limited to the following: Intranet and Internet Sites, Databases, Excel Files,

**A Major Application (MA)** is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunication components. MAs can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Defined in NIST Special Publication 800-18). Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as a "Major Application." Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d).) Examples include, but are not limited to the following: ADB, CAS, CRIS, GemCRIS, NBS, NED, NIHNet, ITAS,

**This individual is considered to be the person who has the most knowledge of the characterization of the IT system who will (in coordination with knowledgeable privacy and security personnel as needed):**

- Work with the IC Privacy Coordinator, ISSO and NIH Senior Official for Privacy to collect information needed to complete PIAs
- Support the completion of PIAs on all NIH systems as required by the Department;
    - Serve as a system manager with working knowledge of the system;

- Serve as PIA point of contact, to whom questions regarding PIAs may be directed;
- Respond to inquires regarding the function, content and disclosure practices of the system;
- Coordinate with appropriate NIH privacy stakeholders to complete PIAs;
- Identify any additional resources needed to complete PIAs;
- Submit completed PIAs to the NIH SOP;
- Update the NIH management on the progress of PIA completion at the request of the NIH SOP;
- Determine adequacy of security controls on NIH systems for operation;
- Consider security controls that protect the privacy of IIF in determining whether NIH systems are allowed to operate;

- Assist in the mitigation of privacy weaknesses identified through the system PIA process into the system Plan of Action and Milestones;
- Maintain responsibility for accuracy of information contained in the PIAs;
- Collaborate with the IC ISSO, Privacy Coordinator, Data Owner, and System/Network Administrator to determine and implement appropriate privacy policies and controls;
- Coordinate with NIH IT personnel to delegate system-level privacy requirements;
- Collect, modify, use, and disclose the minimum PII necessary to complete the mission-related, legally required and/or permitted program task consistent with organizational policy;
- Develop additional system rules of behavior for systems under their responsibility, if rules are not covered under the NIH IT General Rules of Behavior;
- Collaborate with the IC Privacy Coordinator and ISSO to perform risk assessments of the privacy technologies used to secure information in the system;
- Coordinate with IC Privacy Coordinator and ISSO to ensure privacy and security requirements are in place for facilities that process, transmit, or store sensitive information based on the level of privacy risk;
- Coordinate with IC ISSO to establish sensitivity and criticality levels for IC systems and data in accordance with NIST standards and guidelines;
- Assist in the development, activation, and execution of an implementation plan for any new instances of a system-to-system interconnection;
- Ensure PII collected is fulfilling its stated purpose;
- Provide appropriate written privacy notification to individuals whose PII is being collected regarding consent to collect PII prior to its submission, use/disclosure practices of PII prior to its submissions; and major changes that occur to a system that may affect the status or usage of PII contained within that system.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Information Systems Security Officer (ISSO) –** The Institute/Center or Office official who serves as the principal IC contact for coordination, implementation, and enforcement of information-security policies with the NIH CISO and the NIH Senior ISSO.

- Report incidents involving breaches to PII contained in NIH IT systems to the NIH Incident Response Team;
- Ensure proper IT security protection is used to protect PII critical to the program's mission;
- Institute security technologies to ensure the safety of privacy information maintained, stored, and/or transmitted/passed in NIH IT systems;
- Have knowledge of Federal government and Department laws, regulations and policies and procedures regarding privacy;
- Assist the IC Privacy Coordinator and System Owner/Manager in the completion and reviews of Privacy Impact Assessments in answering questions pertaining to security;
- Collaborate with NIH IT business owners to determine appropriate security controls and resources for implementation;
- Coordinate with IC system owners to establish security categorization for IC systems and data in accordance with National Institute of Standards and Technology standards and guidelines;
- Assist the NIH CISO in ensuring that all Federally-mandated information security measures in support of privacy are implemented:
    - enforcing logical access controls that provide privacy protection by preventing unauthorized access, alteration, loss, disclosure;
    - maintaining availability of information and disclosure of information about privacy policies and practices to the public for all applicable IT systems as appropriate;
    - reviewing contracts for systems under NIH CISO control to ensure privacy is appropriately addressed in contract language; and
    - ensuring privacy controls are functioning properly within each IT system and that privacy needs are captured in NIH's plans of action and milestones.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Records Management Officer –** The Institute/Center or Office official who serves as the liaison between IC staff and the NIH Records Management Officer in overseeing the records management program within their IC or Office.

- Provide advisory and support services to IC staff;
- Assist staff in locating the proper records disposition schedule for the records they need to send to the Federal Records Center or National Archives and Records Administration;
- Assist IC staff in the preparation and completion of forms to process records;
- Maintain NIH Records Management Schedule in accordance with NIH Manual Chapters 1742, 1743 and 1744;
- Advise on records retention for Privacy Impact Assessments.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Information Collection Clearance Officer (Project Clearance Liaison) –** The Institute/Center or Office official who serves as the liaison between IC staff and the Office of Management and Budget for OMB clearance functions concerning public information collection activities such as regulations, survey interviews, customer satisfaction surveys, web site questionnaires and epidemiology research.

- Follow Office of Management and Budget requirements when collecting information from 10 or more members of the public;
- Review special requirements for the use of Social Security Numbers;
- Coordinate with the IC Privacy Coordinator, if requested to identify the appropriate Privacy Act Systems of Records Notice to which collected privacy information will belong;
- Submit OMB requests for clearance to the NIH Privacy Act Officer to obtain a memo determining the applicability of the Privacy Act.; and
- Assist the IC Privacy Coordinator and System Owners/Managers, if requested to review Privacy Impact Assessments to determine if an OMB Clearance number is required for the information collected in the IT system.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Website Owner/Administrator –** The Institute/Center or Office official who serves as the principal contact responsible for IC web product development and web project management.

- Identify any additional resources needed to complete machine-readable privacy policies;
- Implement, test, and maintain machine-readable privacy policies and policy reference files;
- Ensure NIH websites are developed in accordance with the NIH Manual Chapters 1745, 1745-1 and 2805;
- Ensure that NIH websites do not employ persistent tracking technologies, of if technologies are in use, ensure that written authorization is issued from the HHS Secretary on an annual basis; and
- Assist IC System Owners/Managers in the review of Privacy Impact Assessments in answering questions related to any websites associated with the IT system.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Contracting/Project Officer –** The Institute/Center or Office official who oversees the development of the documentation and discussions of assigned contracts for award and administration, performs the final review of contract actions, and provides final signature authority.

**Note: Contracting Officers are legally responsible for contracts on behalf of the government. Project Officers do not have the authority to make contractual commitments or change contract terms and conditions.**

- Safeguard the interests of the United States in its contractual relationships;
- Include the Department's privacy considerations in contracts dealing with IT acquisitions;
- Maintain the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring that all privacy terms and conditions of the contract are met;
- Obtain contractual assurances from third parties to ensure that the third party will protect PII in a manner consistent with the privacy practices of the Department and applicable laws and policies, before access to PII is enabled;
- Ensure that the requirements of 1.602-1(b) of the Federal Acquisition Regulation (FAR) have been met, and that sufficient funds are available for obligation. FAR 1.602-1(b) says that no contract shall be entered into unless the contracting officer ensures that all requirements of law, executive orders, regulations, and all other applicable procedures, including clearances and approvals, have been met;
- When the design, development, or operation of a Privacy Act system of records on individuals is required to accomplish an agency function, the Project Officer determines the applicability of the Privacy Act (HHSAR 324.102) and the Contracting Officer inserts the following FAR clauses in solicitations and contracts (both prime and sub-contracts);
    - FAR Clause 52.224-1, Privacy Act Notification
    - FAR Clause 52.224-2, Privacy Act
    - FAR Clause 52.239-1, Privacy and Security Safeguards
    - If a contractor has access to Privacy Act protected information or maintains a system of records on behalf of NIH, Health and Human Services Acquisition Regulation Clause 352.224-70 (Confidentiality of Information) must be added to the prime (and sub) contracts.
- If in the course of executing a government contract, a contractor receives Privacy Act protected information, the Contracting Officer should advise them that the information is protected under the Privacy Act and that the information should be safeguarded;

- If a contractor develops or maintains a Privacy Act system of records on behalf of the federal government, the Contracting Officer should advise that the Privacy Act applies to them to the same extent that it applies to the government, per Section 552a(m) of the Privacy Act;
- If the Privacy Act applies, the contract must:
    - State that the Privacy Act applies;
    - List disclosures a contractor may make;
    - Include a list of the established safeguards;
    - Include procedures to monitor contractor compliance (and identify the federal employee who will serve as the Government monitor);
    - Include a copy of the Privacy Act Systems of Records Notice which must include the items listed above; and
    - Include the contract clauses, as applicable.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

**IC Supervisor –** The Institute/Center or Office official whose position meets the labor management definition of a supervisor as defined in 5 U.S.C. 7103(a)(10).

- Protect personal data at all times;
- Ensure personnel comply with privacy policies and provide the personnel, financial, and physical resources required to protect privacy;
- Ensure that employees complete all required privacy and IT security awareness training within the mandated timeframe;
- Review employee requests for telework to ensure all proper privacy and security measures are in place;
- Consider having telework agreements reviewed by the IC Privacy Coordinator and ISSO to address privacy and/or security concerns;
- Ensure that the Administrative Officer is aware of all employee or contractor separations from duty so they in turn can notify the appropriate IC ISSO and Human Resources point of contact when NIH personnel are separated from the Department;
- Pursue disciplinary actions against personnel who violate the NIH IT General Rules of Behavior and system specific and/or agency rules of behavior;
- Do not share personal data with anyone unless the recipient is listed under the routine uses of disclosure of the Privacy Act Systems of Records Notice or the record subject has given written permission to disclose it;
- Password protect and encrypt personal data placed on shared drives, the Internet or the Intranet drives;
- Issue passwords or authorize access only to those with a valid business need for access;
- Remove personal data once it no longer needs to be posted; and
- Ensure that personal data entered, or accessed in an application or website via the Internet or Intranet is password protected and encrypted.

Primary Role and Responsibilities

All of the primary roles and responsibilities are dependent upon consistent, cooperative and collaborative work with other staff members and customers to ensure an effective privacy program and achieve organizational goals.

## IC Administrative Officer

Notify appropriate IC ISSO and Human Resources point of contact when NIH personnel are separated from the Department.

## IC System User and Employee

- Comply with the Departmental and NIH privacy policies, standards, and procedures;
- Be aware of special privacy requirements for accessing, protecting, handling, and using data;
- Report potential or occurring privacy incidents to the IC ISSO and Privacy Coordinator;
- Seek guidance from supervisors when implementing privacy policies;
- Ensure NIH data is appropriately marked to indicate the sensitivity of the data;
- Ensure sensitivity privacy data is not stored on laptop computers or other portable devices unless they are encrypted with standards commensurate with the sensitive level of the data being used, or otherwise approved through a waiver of the encryption requirement;
- Read, acknowledge, sign, and comply with all privacy requirements in the NIH IT General Rules of Behavior and system-specific rules of behavior before gaining access to government systems and networks;
- Implement specific safeguards to prevent fraud, waste, or abuse of the systems, networks, and data authorized to use;
- Agree to not disable, remove, install with intent to bypass, or otherwise alter privacy settings or administrative settings designed to protect privacy controls on NIH IT resources; and
- Complete all required NIH privacy awareness and IT security awareness training.